IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	
Adrian Patrick Kent, *et al.*	Confirmation No: 2520
Serial No.: 10/627,158	Group Art Unit: 2137
Filed: July 25, 2003	Examiner: Popham, Jeffrey D.
For: Improvements Relating to Quantum Cryptography	Atty. Docket No.: 200206289-1

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed November 13, 2007, responding to the final Office Action mailed July 13, 2007.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1-49 stand finally rejected. No claims have been allowed. The rejections of claims 1-49 are appealed.

IV. Status of Amendments

This application was originally filed on July 25, 2003, with forty-nine (49) claims. In a Response filed April 26, 2007, Applicants amended claims 1, 25, 26, and 35. The claims in the attached Claims Appendix (see below) reflect the present state of Applicants' claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel (Figure 1, 16). The method comprises generating a plurality of random quantum states of a quantum entity. Each random state is defied by a randomly selected one of a first plurality of bases in Hilbert space. The first plurality of bases is randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space. Applicants' specification, page 18, lines 14-16. The method further comprises transmitting the plurality of random quantum states of the quantum entity via the quantum channel (Figure 1, 16) to the recipient, Applicants' specification, page 13, lines 27-30, and measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space. Applicants' specification, page 13, lines 32-33. The second plurality of bases is randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space. Applicants' specification, page 18 lines 30-33. The method further comprises transmitting to the recipient composition information describing a subset of the

plurality of random quantum states and analyzing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states. Applicants' specification, page 19, lines 11-31. Such a method comprises establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar, Applicants' specification, pages 19-20, lines 29-71; deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset, Applicants' specification, page 21, lines 13-19; and carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings. Applicants' specification, page 22, lines 24-32.

Embodiments according to independent claim 26 describe a method of a sender establishing a secret random cryptographic key shared with a recipient using a quantum communications channel (Figure 1, 16). The method comprises generating a plurality of random quantum states of a quantum entity. Applicants' specification, page 18, lines 12-16. Each random state is defined by a randomly selected one of a first plurality of bases in Hilbert space. The first plurality of bases is randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space. Applicants' specification, page 18, lines

14-16. The method further comprises transmitting the plurality of random quantum states of the quantum entity via the quantum channel (Figure 1, 16) to the recipient, Applicants' specification, page 13, lines 27-30; transmitting to the recipient composition information describing a subset of the plurality of random quantum states, Applicants' specification, page 19, lines 11-31; and deriving a first binary string from the transmitted plurality of quantum states not in the subset. Applicants' specification, page 21, lines 13-19. Such a method further comprises using error correction techniques to establish the shared secret random cryptographic key from the first binary string. Applicants' specification, page 22, lines 24-32.

Embodiments according to independent claim 35 describe a method of a recipient establishing a secret random cryptographic key shared with a sender using a quantum communications channel (Figure 1, 16). The method comprises receiving a plurality of random quantum states of a quantum entity via the quantum channel (Figure 1, 16) from the sender, Applicants' specification, page 13, lines 27-32, and measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space. Applicants' specification, page 13, lines 32-33. The second plurality of bases is randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space. Applicants' specification, page 18 lines 30-33. The method further comprises receiving from the sender composition information describing a subset of the plurality of random quantum states and analyzing the received composition

information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states. Applicants' specification, page 19, lines 11-31. Such a method further comprises establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar, Applicants' specification, pages 19-20, lines 29-71; deriving a recipient binary string from the received plurality of quantum states not in the subset, Applicants' specification, page 21, lines 13-19; and using error correction techniques to establish the shared secret random cryptographic key from the recipient binary string. Applicants' specification, page 22, lines 24-32.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-7, 10-13, 16-20, 22-24, 26-38, 41-43, and 46-49 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Bennett* ("Experimental Quantum Cryptography," September, 1991, pages 1-28) in view of *Sych* ("Quantum Cryptography with Continuous Alphabet," April 4, 2003, pages 1-14).

Claims 8, 9, 21, 25, 39, and 40 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Bennett* in view of *Sych* in further view of

Black ("Quantum Computing and Communication," February 20, 2002, pages 1-52).

Claims 14, 15, 44, and 45 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Bennett* in view of *Sych* in further view of *Franson* (U.S. Patent No. 6,678,450.

VII. Arguments

A. Claims 1-7, 10-13, 16-20, 22-24, 26-38, 41-43, and 46-49

Claims 1-7, 10-13, 16-20, 22-24, 26-38, 41-43, and 46-49 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Bennett* ("Experimental Quantum Cryptography," September, 1991, pages 1-28) in view of *Sych* ("Quantum Cryptography with Continuous Alphabet," April 4, 2003, pages 1-14). Applicants respectfully traverse this rejection.

1. The *Bennett* Reference

Bennett describes a quantum key distribution protocol where a sender ("Alice") sends a random sequence of photons polarized horizontal, vertical, right-circular, and left-circular. A recipient ("Bob") measures the photons' polarization in a random sequence of bases, rectilinear and circular and records the results. Bob tells Alice which basis he used for each photon he received and Alice tells him which bases were correct. Alice and Bob keep only the data from these correctly-measured photons and discard the rest. The remaining cases

are then translated into bits (1's and 0's) and thereby become a key. *See* page 5. Accordingly, the approach described in *Bennett* has the underlying requirement of needing to know which basis are correct amongst the transmissions.

2. The *Sych* Reference

Sych describes a quantum key distribution protocol which uses an alphabet including all of the states of the Hilbert space. *See* page 5. *Sych* describes that bases reconciliation may be performed to improve performance. *See* page 8 and Figure 2.

3. Applicants' Claim 1

Applicants' independent claim 1 provides as follows:

> A method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method comprising:
>
> generating a plurality of random quantum states of a quantum entity, each random state being defied by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;
>
> transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;
>
> measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;
>
> ***transmitting to the recipient composition information describing a subset of the plurality of random quantum states;***
>
> ***analysing the received composition information and the measured quantum states corresponding to the subset to***

derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;

establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;

deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset; and

carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings.

(Emphasis added).

Bennett in view of *Sych* describes a method of quantum cryptography where photons may be transmitted to a recipient and a reconciliation process is used to match the basis of measurement used by the recipient for a photon with the basis used to transmit the photon. Both *Bennett* and *Sych* disclose the reconciliation technique of identifying a string of qubits on which the recipient carried out measurements in a basis containing the qubit prepared by the sender. Diversely, in claim 1, the claimed method describes "transmitting to the recipient composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are

sufficiently similar; [and] deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset." This approach is not taught or suggested by the cited art.

For example, *Bennett* describes a quantum key distribution protocol where a sender ("Alice") sends a random sequence of photons polarized horizontal, vertical, right-circular, and left-circular. A recipient ("Bob") measures the photons' polarization in a random sequence of bases, rectilinear and circular and records the results. Bob tells Alice which basis he used for each photon he received and Alice tells him which bases were correct. Alice and Bob keep only the data from these correctly-measured photons and discard the rest. The remaining cases are then translated into bits (1's and 0's) and thereby become a key. *See* page 5. As such, *Bennett* does not disclose that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states. *Bennett* also does not describe that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar. Likewise, *Bennett* does not disclose that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset. For example, in *Bennett*, photons in a subset that were verified to be correctly measured using basis reconciliation are used to determine a key and the rest are

discarded. For at least these reasons, *Bennett* fails to teach or suggest "transmitting to the recipient composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset," as recited in claim 1.

Similarly, *Sych* describes that a similar technique for basis reconciliation may be used to improve performance of quantum cryptography. However, *Sych* does not disclose that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states. *Sych* also does not describe that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar. Likewise, *Sych* does not disclose that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset. For at least these reasons,

Sych individually or in combination with *Bennett* fails to teach or suggest "transmitting to the recipient composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset," as recited in claim 1.

Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Bennett* in view of *Sync* has not been made, and the rejection of claim 1 should be overturned.

4. Applicants' Claims 2-7, 10-13, 16-20, and 22-24

Dependent claims 2-7, 10-13, 16-20, and 22-24 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that dependent claims 2-7, 10-13, 16-20, and 22-24 contain all the features of allowable independent claim 1. For at least this reason, the rejections of claims 2-7, 10-13, 16-20, and 22-24 should be overturned.

5. Applicant's Claim 26

As provided in independent claim 26, Applicants claim:

> A method of a sender establishing a secret random cryptographic key shared with a recipient using a quantum communications channel, the method comprising:
>
> generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;
>
> transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;
>
> ***transmitting to the recipient composition information describing a subset of the plurality of random quantum states;***
>
> ***deriving a first binary string from the transmitted plurality of quantum states not in the subset;*** and
>
> using error correction techniques to establish the shared secret random cryptographic key from the first binary string.

(Emphasis added).

Bennett in view of *Sych* describes a method of quantum cryptography where photons may be transmitted to a recipient and a reconciliation process is used to match the basis of measurement used by the recipient for a photon with the basis used to transmit the photon. Both *Bennett* and *Sych* disclose the reconciliation technique of identifying a string of qubits on which the recipient carried out measurements in a basis containing the qubit prepared by the sender. Diversely, in claim 26, the claimed method describes "transmitting to the recipient composition information describing a subset of the plurality of random quantum states; [and] deriving a first binary string from the transmitted plurality of quantum states not in the subset." This approach is not taught or suggested by the cited art.

For example, *Bennett* describes a quantum key distribution protocol where a sender ("Alice") sends a random sequence of photons polarized horizontal, vertical, right-circular, and left-circular. A recipient ("Bob") measures the photons' polarization in a random sequence of bases, rectilinear and circular and records the results. Bob tells Alice which basis he used for each photon he received and Alice tells him which bases were correct. Alice and Bob keep only the data from these correctly-measured photons and discard the rest. The remaining cases are then translated into bits (1's and 0's) and thereby become a key. *See* page 5. As such, *Bennett* does not disclose that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states. *Bennett* also does not describe that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar. Likewise, *Bennett* does not disclose that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset. For example, in *Bennett*, photons in a subset that were verified to be correctly measured using basis reconciliation are used to determine a key and the rest are discarded. For at least these reasons, *Bennett* fails to teach or suggest "transmitting to the recipient composition information describing a subset of the plurality of random quantum states [and] deriving a first binary string from the transmitted plurality of quantum states not in the subset," as recited in claim 26.

Similarly, *Sych* describes that a similar technique for basis reconciliation may be used to improve performance of quantum cryptography. However, *Sych* does not disclose that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states. *Sych* also does not describe that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar. Likewise, *Sych* does not disclose that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset. For at least these reasons, *Sych* individually or in combination with *Bennett* fails to teach or suggest "transmitting to the recipient composition information describing a subset of the plurality of random quantum states [and] deriving a first binary string from the transmitted plurality of quantum states not in the subset," as recited in claim 26.

Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Bennett* in view of *Sync* has not been made, and the rejection of claim 26 should be overturned.

6. Applicants' Claims 27-34

Dependent claims 27-34 (which depend from independent claim 26) are allowable as a matter of law for at least the reason that dependent claims 27-34

contain all the features of allowable independent claim 26. For at least this reason, the rejections of claims 27-34 should be overturned.

7. Applicants' Claim 35

As provided in independent claim 35, Applicants claim:

> A method of a recipient establishing a secret random cryptographic key shared with a sender using a quantum communications channel, the method comprising:
> receiving a plurality of random quantum states of a quantum entity via the quantum channel from the sender;
> measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;
> ***receiving from the sender composition information describing a subset of the plurality of random quantum states;***
> ***analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;***
> ***establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;***
> ***deriving a recipient binary string from the received plurality of quantum states not in the subset;*** and
> using error correction techniques to establish the shared secret random cryptographic key from the recipient binary string.

(Emphasis added).

Bennett in view of *Sych* describes a method of quantum cryptography where photons may be transmitted to a recipient and a reconciliation process is used to match the basis of measurement used by the recipient for a photon with

the basis used to transmit the photon. Both *Bennett* and *Sych* disclose the reconciliation technique of identifying a string of qubits on which the recipient carried out measurements in a basis containing the qubit prepared by the sender. Diversely, in claim 35, the claimed method describes "receiving from the sender composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving a recipient binary string from the received plurality of quantum states not in the subset." This approach is not taught or suggested by the cited art.

For example, *Bennett* describes a quantum key distribution protocol where a sender ("Alice") sends a random sequence of photons polarized horizontal, vertical, right-circular, and left-circular. A recipient ("Bob") measures the photons' polarization in a random sequence of bases, rectilinear and circular and records the results. Bob tells Alice which basis he used for each photon he received and Alice tells him which bases were correct. Alice and Bob keep only the data from these correctly-measured photons and discard the rest. The remaining cases are then translated into bits (1's and 0's) and thereby become a key. *See* page 5. As such, *Bennett* does not disclose that a statistical distribution is derived

from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states. *Bennett* also does not describe that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar. Likewise, *Bennett* does not disclose that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset. For example, in *Bennett*, photons in a subset that were verified to be correctly measured using basis reconciliation are used to determine a key and the rest are discarded. For at least these reasons, *Bennett* fails to teach or suggest "receiving from the sender composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving a recipient binary string from the received plurality of quantum states not in the subset," as recited in claim 35.

Similarly, *Sych* describes that a similar technique for basis reconciliation may be used to improve performance of quantum cryptography. However, *Sych*

does not disclose that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states. *Sych* also does not describe that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar. Likewise, *Sych* does not disclose that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset. For at least these reasons, *Sych* individually or in combination with *Bennett* fails to teach or suggest "receiving from the sender composition information describing a subset of the plurality of random quantum states; analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states; establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar; [and] deriving a recipient binary string from the received plurality of quantum states not in the subset," as recited in claim 35.

Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Bennett* in view of *Sync* has not been made, and the rejection of claim 35 should be overturned.

8. Applicants' Claims 36-38, 41-43, and 46-49

Dependent claims 36-38, 41-43, and 46-49 (which depend from independent claim 35) are allowable as a matter of law for at least the reason that dependent claims 36-38, 41-43, and 46-49 contain all the features of allowable independent claim 35. For at least this reason, the rejections of claims 36-38, 41-43, and 46-49 should be overturned.

B. Claims 8, 9, 21, 25, 39, and 40

Claims 8, 9, 21, 25, 39, and 40 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Bennett* in view of *Sych* in further view of *Black* ("Quantum Computing and Communication," February 20, 2002, pages 1-52).

All of the features of allowable independent claims 1, and 35 are not taught and suggested by *Bennett* and *Sync*, as previously discussed. Further, the cited art of *Black* fails to cure the deficiencies of the *Bennett* and *Sych* references in suggesting or teaching all of the claimed features in claims 1 and 35. Further, claims 8, 9, 21, 25, 39, and 40 recite additional features. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Bennett* in view of *Sych* in further view of *Black* has not been made, and the rejections of claims 8, 9, 21, 25, 39, and 40 should be overturned.

C. Claims 14, 15, 44, and 45

Claims 14, 15, 44, and 45 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Bennett* in view of *Sych* in further view of *Franson* (U.S. Patent No. 6,678,450).

All of the features of allowable independent claims 1, and 35 are not taught and suggested by *Bennett* and *Sync*, as previously discussed. Further, the cited art of *Franson* fails to cure the deficiencies of the *Bennett* and *Sych* references in suggesting or teaching all of the claimed features in claims 1 and 35. Further, claims 14, 15, 44, and 45 recite additional features. Therefore, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Bennett* in view of *Sych* in further view of *Franson* has not been made, and the rejections of claims 14, 15, 44, and 45 should be overturned.

VIII. Conclusion

In summary, it is Applicants' position that Applicants' claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicants' pending claims.

Respectfully submitted,

By: 
Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method comprising:

generating a plurality of random quantum states of a quantum entity, each random state being defied by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;

transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;

measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;

transmitting to the recipient composition information describing a subset of the plurality of random quantum states;

analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;

establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;

deriving, a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset; and

carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings.

2. A method according to claim 1, wherein the first and second plurality of bases in Hilbert space each comprise at least four random bases.

3. A method according to claim 1, wherein the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space.

4. A method according to claim 1, wherein the selecting step comprises generating and measuring a first plurality of bases in a real subspace of two-dimensional Hilbert space.

5. A method according to claim 1, wherein the composition information transmitting step comprises transmitting information describing the bases of the subset of the plurality of random quantum states.

6. A method according to claim 1, wherein the analysing step comprises analysing the information describing the bases to derive the first statistical distribution.

7. A method according to claim 1, wherein the establishing step comprises determining a statistical error rate.

8. A method according to claim 1, wherein the establishing step comprises:

determining the degree of difference between the first and second statistical distributions; and

accepting the security of the channel if the degree of correlation between the two distributions is greater than a threshold level.

9. A method according to claim 8, further comprising selecting the value of the threshold level.

10. A method according to claim 1, wherein the subset information transmitting step comprises transmitting the subset information over a public channel, such as a radio channel.

11. A method according to claim 1, wherein the deriving step comprises transmitting information to the recipient representing the bases for the quantum states not in the subset which make up the first binary string.

12. A method according to claim 1, wherein the carrying out the reconciliation step comprises using privacy amplification techniques.

13. A method according to claim 1, wherein the quantum entity is photons and the quantum states are degrees of polarisation of the photons.

14. A method according to claim 1, further comprising temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step.

15. A method according to claim 14, wherein the measuring step is carried out after the temporary storing step and uses the received recipient composition information to determine some of the bases of the second plurality of bases.

16. A method according to claim 1, further comprising determining the second plurality of bases independently of the first plurality of bases.

17. A method according to claim 1, wherein the first and second pluralities of bases are selected randomly.

18. A method according to claim 1, further comprising the recipient transmitting some information about the bases chosen for measurement and/or the measurement results to the sender.

19. A method according to claim 1, wherein the step of carrying out the reconciliation comprises using several quantum states to generate a single bit of the shared secret key at both the sender and recipient.

20. A method according to claim 1, further comprising transmitting data regarding the second statistical distribution from the recipient to the sender.

21. A method according to claim 1, further comprising determining the size of the secret shared key to be of the same order as the size of a message to be encrypted with the key.

22. A method according to claim 1, wherein each of the plurality of random quantum states define two-dimensional information describing the condition of the quantum entity.

23. A method according to claim 1, wherein each of the plurality of random quantum states define n-dimensional information describing the condition of the quantum entity, where n is three or more.

24. A method according to claim 1, wherein the plurality of random quantum states are arranged geometrically to be uniformly separated within Hilbert space.

25. A secure communications method for conveying a message from a sender to an intended recipient, the method comprising:

establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel according to a method as described in claim 1;

using the shared secret key as a one-time pad for secure encryption of the elements of the message at the sender;

transmitting the encrypted message to the intended recipient using a conventional communications channel; and

using the shared secret key as a one-time pad for secure decryption of the encrypted elements of the message at the recipient.

26. A method of a sender establishing a secret random cryptographic key shared with a recipient using a quantum communications channel, the method comprising:

generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space, the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;

transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient;

transmitting to the recipient composition information describing a subset of the plurality of random quantum states;

deriving a first binary string from the transmitted plurality of quantum states not in the subset; and

using error correction techniques to establish the shared secret random cryptographic key from the first binary string.

27. A method according to claim 26, wherein the first plurality of bases in Hilbert space comprises at least four random bases.

28. A method according to claim 26, wherein the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space.

29. A method according to claim 26, wherein the selecting step comprises generating and measuring a first plurality of bases in a real subspace of two-dimensional Hilbert space.

30. A method according to claim 26, wherein the composition information transmitting step comprises transmitting information describing the bases of the subset of the plurality of random quantum states.

31. A method according to claim 26, wherein the subset information transmitting step comprises transmitting the subset information over a public channel, such as a radio channel.

32. A method according to claim 26, wherein the quantum entity is photons and the quantum states are degrees of polarisation of the photons.

33. A method according to claim 26, wherein the first plurality of bases is selected randomly.

34. A method according to claim 26, wherein the step of using error correction techniques comprises using several quantum states to generate a single bit of the shared secret key at the sender.

35. A method of a recipient establishing a secret random cryptographic key shared with a sender using a quantum communications channel, the method comprising:

receiving a plurality of random quantum states of a quantum entity via the quantum channel from the sender;

measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space, the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space;

receiving from the sender composition information describing a subset of the plurality of random quantum states;

analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;

establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;

deriving a recipient binary string from the received plurality of quantum states not in the subset; and

using error correction techniques to establish the shared secret random cryptographic key from the recipient binary string.

36. A method according to claim 35, wherein the recipient's plurality of bases

in Hilbert space comprises at least four random bases.

37. A method according to claim 35, wherein the analysing step comprises analysing the information describing the bases to derive the first statistical distribution.

38. A method according to claim 35, wherein the establishing step comprises determining a statistical error rate.

39. A method according to claim 35, wherein the establishing step comprises:

determining the degree of difference between the fist and second statistical distributions; and

accepting the security of the channel if the degree of correlation between the two distributions is greater than a threshold level.

40. A method according to claim 39, further comprising selecting the value of the threshold level.

41. A method according to claim 35, wherein the deriving step comprises transmitting information to the recipient representing the bases for the quantum states not in the subset which make up the first binary string.

42. A method according to claim 35, wherein the carrying out the reconciliation step comprises using privacy amplification techniques.

43. A method according to claim 35, wherein the quantum entity is photons and the quantum states are degrees of polarisation of the photons.

44. A method according to claim 35, further comprising temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step.

45. A method according to claim 44, wherein the measuring step is carried out after the temporary storing step and uses the received recipient composition information to determine some of the bases of the second plurality of bases.

46. A method according to claim 35, wherein the recipient's plurality of bases is selected randomly.

47. A method according to claim 35, further comprising the recipient transmitting some information about the bases chosen for measurement and/or the measurement results to the sender.

48. A method according to claim 35, wherein the step of using error correction techniques comprises using several quantum states to generate a single bit of the shared secret key at the recipient.

49. A method according to claim 35, further comprising transmitting data regarding the second statistical distribution from the recipient to the sender.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.